Disaster Preparedness: Taking Care of Your People and Your Data

ALA – Annual Conference
April 15, 2019

Kathy Scourby    David Constantine

DEFINITION OF DISASTER OR CRISIS

“Any situation that threatens the integrity or reputation of a firm or business, usually brought on by adverse or negative media attention.”
## Disaster Statistics

<table>
<thead>
<tr>
<th>50%</th>
<th>3yrs.</th>
<th>Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>50% (or more) of businesses that experience a major disaster will never return to the marketplace.</td>
<td>Of those that survive a major disaster, 50% (or more) will file bankruptcy within 3 years. (Chubb)</td>
<td>Those that survive are prepared to meet their clients’ needs By planning/preparing to react to a disaster.</td>
</tr>
</tbody>
</table>

"By the time you hear the thunder, it is too late to build the ark." (Anonymous)

---

### 2017/2018 Major Crises

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Parkland School Shooting</td>
<td>Under Armour - My Fitness Pal 150 million accts exposed March/2018</td>
</tr>
<tr>
<td>Parkland, FL February/2018</td>
<td>Jason's Deli 3.4 million accounts exposed January/2018</td>
</tr>
<tr>
<td>Borderline Club &amp; Synagogue Shooting</td>
<td>Sacramento Bee Newspaper 19.4 million accts exposed February/2018</td>
</tr>
<tr>
<td>CA and PA Oct &amp; Nov/2018</td>
<td>Suntrust Bank 1.5 million accts exposed April/2018</td>
</tr>
<tr>
<td>United Airlines, Southwest Airlines and Starbucks</td>
<td>Marriott (Starwood) 500 million accts exposed November/2018</td>
</tr>
<tr>
<td>April/2017</td>
<td></td>
</tr>
<tr>
<td>Civil Unrest</td>
<td>Saks &amp; Lord &amp; Taylor 5 million accts exposed April/2018</td>
</tr>
<tr>
<td>Charlottesville, VA August/2017</td>
<td></td>
</tr>
<tr>
<td>Hurricanes Florence, Michael, Harvey, Irma, Maria North Carolina, Texas, Florida &amp; PR August &amp; Sept 2017/2018</td>
<td></td>
</tr>
<tr>
<td>Wild Fires – Camp Fire, Woolsey Fire &amp; Vineyard Fires California Oct/2017 &amp; Nov/2018</td>
<td></td>
</tr>
<tr>
<td>Earthquake &amp; Tsunami Indonesia &amp; Alaska Sept &amp; Nov/2018</td>
<td></td>
</tr>
</tbody>
</table>

---

### 2017/2018 Major Crises

- Parkland School Shooting, Parkland, FL, February/2018
- Borderline Club & Synagogue Shooting, CA and PA, October & November 2018
- United Airlines, Southwest Airlines, and Starbucks, April 2017
- Civil Unrest, Charlottesville, VA, August 2017
- Hurricanes Florence, Michael, Harvey, Irma, Maria, North Carolina, Texas, Florida & PR, August & September 2017/2018
- Wild Fires – Camp Fire, Woolsey Fire & Vineyard Fires, California, October/2017 & November/2018
- Earthquake & Tsunami, Indonesia & Alaska, September & November 2018
- Under Armour - My Fitness Pal, 150 million accounts exposed, March 2018
- Jason's Deli, 3.4 million accounts exposed, January 2018
- Sacramento Bee Newspaper, 19.4 million accounts exposed, February 2018
- Suntrust Bank, 1.5 million accounts exposed, April 2018
- Marriott (Starwood), 500 million accounts exposed, November 2018
- Saks & Lord & Taylor, 5 million accounts exposed, April 2018
It is not a question of “IF”, but “WHEN”

1. Potential Violation of Ethical Rules
2. Potential Professional Negligence Liability
3. Potential loss of Revenue, Reputation & Clients

“RESOLVED, That the American Bar Association urges all lawyers to regularly assess their practice environment to identify and address risks that arise from any natural or manmade disaster that may compromise their ability to diligently and competently protect their clients’ interests, and maintain the security of their clients’ property.”

- ABA Resolution 116 (adopted August 8-9, 2011)
COMMITTEE ON DISASTER RESPONSE & PREPAREDNESS

Includes information:
- A Lawyer’s Guide to Disaster Planning
- Preparing Law Firms and Clients for Issues in Cyberspace
- Formal Opinion 477R (4/11/17)
- Formal Opinion 482 (09/19/18)
- Formal Opinion 483 (10/17/18)

Ethical Obligations Related to Disasters
- Model Rule 1.1 (Competence)
- Model Rule 1.3 (Diligence)
- Model Rule 1.4 (Communication)
- Model Rule 1.6 (Confidentiality)
- Model Rule 1.15 (Safekeeping Property)
- Model Rule 1.16 (Termination of Representation)
- Model Rule 5.5 (Multijurisdictional Practice)
- Model Rule 7.1 – 7.3 (Limiting Advertising directed to and solicitation of disaster victims)
**NEED FOR A COMPREHENSIVE BUSINESS CONTINUITY PLAN**

<table>
<thead>
<tr>
<th>Compliance issues (Client audits and RFP's)</th>
<th>Facility and/or personnel changes/moves/relocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory Requirements (government or ISO certification)</td>
<td>Changes in voice/data networks</td>
</tr>
<tr>
<td>New hardware, operating systems or applications in place</td>
<td>Changes in critical third party vendor/suppliers</td>
</tr>
<tr>
<td></td>
<td>Hackers, Malware &amp; Viruses</td>
</tr>
</tbody>
</table>

**CRISIS MANAGEMENT TEAM**

- Consider size of business/office to determine how many members for team
- Key Admin players in the office and a back-up teammate for each member
- People who are willing to volunteer time
- People who will be calm and authoritative in an emergency situation
- Specific/separate crisis communication team
Bring knowledge and expertise together to deal with major events that threaten the ability of your firm to perform its mission (service to clients).

Gather information quickly about what is happening.

Share that information efficiently among the team’s members.

ROLES AND RESPONSIBILITIES OF CRISIS TEAMS IN ALL FIRMS

Decide on an immediate course of action for a given problem, or send the information necessary to senior management for a decision on the problem.

Identify and direct resources to carry out the decisions.

Monitor how effectively those decisions are being carried out, adjusting direction as necessary.
TRAINING OF
CRISIS MANAGEMENT TEAM

Consistent training for all Crisis Team members is essential

- Actual Drills
- Webinars
- Meetings
- Hacking & Malware Simulations
- Face-to-Face/On-Line Training
- Table Top Exercises
- Exercises

TYPES OF DRILLS

- Recovery From Back Up Drills
- Data Breach Drills
- Active Assailant Drills
- Evacuation Drills
- Shelter-in-Place Drills
- Physical Building Security Drills
**Types of Drills**

- Recovery from Back Up Drills
- Evacuation Drills
- Shelter-In-Place Drills
- Active Assailant Drills
- Data Breach Drills
- Physical Building Security & Other Drills

---

**Long Before The Day You Get Hacked**

- Written Internal Plan for data security
- Written Emergency Mode Operations Plan
- Text & Email Groups - secure file area in the cloud.
- Information Security Training
- Information Security Reference Cards for users
**Images, Backups & Priorities**

- Air-Gapped Backup and Server image storage
- Critical Firm Documents in the cloud
- Emergency payroll plans and duplicate paper checks for client expenses
- All Firm Admin passcodes/ hints in a private cloud account, accessible via smartphones.
- Push out Attorney Cell numbers to clients

**Interim Crisis Operations**

- Can your IT provider make your server images live on their servers?
- Can all of your attorneys access their email remotely? Do they all have active signatures?
- Will copiers operate offline? Printers?
- Without a standby or Hot site location, know what servers you have and what model you need should replacement be required?
ASSess Vulnerability of Your Data

Perform a Risk Assessment using NIST standards as a minimum.

Proceed with Independent Vulnerability scans of your servers and workstations at least annually

Verify that software patches are current and applied in a timely manner every month.

Force a restore of some random data set or file or folders once a month.

HI PAA
Four Things Required

Put #1 Safeguards in place to protect PHI

Limit #2 access to PHI or sensitive information to only those with a “need to know”

Have #3 written agreements with those who create, control, access or store PHI

#4 Written procedures with annual user training

Document...Document...Document
STATE OF READINESS OF YOUR BCP

1. Necessary/required resources in place through testing – the need for resiliency

2. Assess critical business functions – conduct a Business Impact Assessment (BIA)

3. IS COMPLIANCE NECESSARY??? ...reasons to test?

4. Testing, Testing, Testing!!!

RESILIENCE & RECOVERY

Preparedness (actions taken to promote readiness)

Mitigation (reduce risk)

Response (actions taken to save life/property)

Recovery (actions taken to restore & resume operations)
Bring up a business card to receive

Links and references to a variety of helpful documents including forms and templates via email following the conference.

QUESTIONS?

Kathryn (Kathy) Scourby, CBCP
KNS Consulting, LLC
(865) 789-7694
knscourby@gmail.com

David P. Constantine
Information Security & Compliance
Logical Computer Solutions, Inc.
(251) 510-8215
david@logicalus.com

Presentation may not be used or reproduced without permission – KNS Consulting, LLC

Presentation may not be used or reproduced without permission – KNS Consulting, LLC
YOUR OPINION MATTERS!
Please take a moment now to evaluate this session.
Thank You!